AMENDMENTS TO THE CLAIMS

Claim 1 (currently amended): A method of transferring data in a peer-to-peer computer network that includes a first peer node and a second peer node, the method comprising:

providing the second peer node a location information of an interception node instead of a location information of the first peer node in a data transfer between the first peer node and the second peer node;

establishing a communication channel between the interception node and the second peer node;

receiving the data in the interception node; and

processing the data in the interception node.

Claim 2 (original): The method of claim 1 wherein the data are received by the interception node from the second peer node.

Claim 3 (original): The method of claim 1 further comprising:

establishing a communication channel between the interception node and the first peer node; and

wherein the data are received by the interception node from the first peer node.

Claim 4 (original): The method of claim 1 wherein the data comprise a file.

Claim 5 (original): The method of claim 1 wherein the location information of the first peer node comprises an IP address and a port number.

Claim 6 (original): The method of claim 1 wherein processing the data in the interception node comprises scanning the data for computer viruses.

Claim 7 (original): The method of claim 1 wherein processing the data in the interception node comprises filtering the content of the data.

Claim 8 (original): The method of claim 1 further comprising:

transferring the data from the interception node to the second peer node after the data have been processed in the interception node.

Claim 9 (original): The method of claim 1 further comprising:

transferring the data from the interception node to the first peer node after the data have been processed in the interception node.

Claim 10 (original): A method of transferring a file in a peer-to-peer computer network, the method comprising:

redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

processing the file in the interception node; and

transferring the file from the interception node to the second peer node.

Claim 11 (original): The method of claim 10 wherein the peer-to-peer computer network includes the Internet.

Claim 12 (original): The method of claim 10 wherein processing the file in the interception node comprises scanning the file for viruses.

Claim 13 (original): The method of claim 10 wherein processing the file in the interception node comprises filtering a content of the file.

Claim 14 (original): The method of claim 10 wherein redirecting the file comprises:

informing the second peer node that an address of the first peer node is that of the interception node.

Claim 15 (original): The method of claim 10 wherein transferring the file from the interception node to the second peer node comprises:

querying a P2P server for location information of peer nodes involved in a transfer of the file;

based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node; and

transferring the file from the interception node to the second peer node.

Claim 16 (original): A system for transferring data in a peer-to-peer network, the system comprising:

a presence modifier configured to detect a publication of a location information of a first peer node, the presence modifier being configured to provide to a second peer node a location information of an interception node instead of the location information of the first peer node in response to a detection of the publication, the first peer node and the second peer node being computers in the peer-to-peer computer network.

Claim 17 (original): The system of claim 16 further comprising:

a data scanner in the interception node, the data scanner being configured to scan data passing through the interception node.

Claim 18 (currently amended): The system of claim 16 wherein the interception node comprises a computer that is separate from ~~the~~ a P2P server.

Claim 19 (original): The system of claim 16 wherein the location information of the first peer node comprises an IP address and a port number.

Claim 20 (original): The system of claim 17 wherein the data scanner is configured to scan the data for computer viruses.

Claim 21 (currently amended): The system of claim 16 further comprising:

~~of was of~~ a transfer manager in the interception node, the transfer manager being configured to obtain session information from the presence modifier.

Claim 22 (original): A method of transferring a file in a peer-to-peer computer network, the method comprising:

transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

scanning the file for viruses in the interception node; and

transferring the file from the interception node to the second peer node.